

Preparando a su organización para la nueva era de la ciberseguridad

La LOFC ya está vigente

Ecuador cuenta con un marco integral de **ciberseguridad**. Alcanza a entidades de los sectores público y privado que son responsables de operar infraestructura crítica digital que soporta servicios esenciales y a los Prestadores de Servicios Digitales.

Sectores actualmente alcanzados

- Sistema financiero
- Salud y seguridad social
- Educación
- Energía
- Telecomunicaciones
- Agua y saneamiento
- Transporte y vialidad
- Puertos y aeropuertos
- Hidrocarburos
- Recursos naturales no renovables
- Biodiversidad y patrimonio genético

Servicios digitales

Procesamiento, almacenamiento, transmisión, intermediación o seguridad de datos y sistemas. Incluye servicios en la nube, centros de datos, pasarelas de pago y plataformas de intermediación.

Desafíos y oportunidades de la LOFC

01

Alcance y regulación

Determinar si aplica como: operador de infraestructura crítica digital, Prestador de Servicio Digital (PSD), proveedor de tecnología indispensable o está incluida en el Catálogo Nacional de Servicios Esenciales e Infraestructura Crítica Digital.

02

Gobierno y gestión de riesgos

Definir roles, supervisión ejecutiva y métricas, conectando riesgos cibernéticos, activos críticos e implementado procesos y controles de seguridad.

03

Incidentes y resiliencia

Fortalecer la detección, el escalamiento y la notificación de incidentes dentro del plazo aplicable, y asegurar la continuidad de servicios esenciales.

04

Terceros y pruebas de seguridad

Gestionar proveedores críticos y servicios digitales, y alinear las pruebas de seguridad y Ethical Hacking con el nuevo marco.

Tres datos que ponen la regulación en perspectiva

72 h

Notificación de incidentes de ciberseguridad

1,5%

Sanción máxima sobre volumen de negocio, según gravedad.

6 meses

Plazo de MINTEL para emitir los reglamentos clave; vence en nov 2026.

¿Está preparada su organización?

01 Sector financiero ¿Su órgano de control fija los estándares y el canal de reporte de incidentes?	02 Salud y seguridad social ¿Sus servicios esenciales y datos personales tienen continuidad y respuesta probadas?	03 Energía, telecom. y transporte ¿Sus sistemas OT y redes críticas están clasificados y protegidos?	04 PSD y proveedores de tecnología ¿Puede demostrar a sus clientes un SGSI y controles efectivos?	05 Sector público ¿Tiene gobierno, punto de contacto 24/7 y capacidad de notificar a tiempo?
---	---	--	---	--

Enfoque de PwC



Nuestros servicios

Diagnóstico de aplicabilidad LOFC Conclusión de aplicabilidad (sector crítico o PSD), obligaciones frente a clientes regulados y mapa preliminar.	01	Cybersecurity Gap Assessment Matriz de brechas, quick wins y hoja de ruta priorizada.	02	Gobierno, riesgos y resiliencia Implementación de sistemas de gestión de ciberseguridad (ISO 27001, NIST CSF) y plan de recuperación de desastres.	03
Preparación y respuesta a incidentes Protocolos, playbooks, simulaciones y criterios de notificación.	04	Capacidades complementarias Ethical Hacking, gestión de terceros, cloud, IAM, vulnerabilidades, cultura cyber y servicios gestionados de ciberseguridad.	05	Acompañamiento de implementación Asesoría para ejecutar, monitorear y mejorar las capacidades priorizadas.	06

Conversemos sobre el primer paso para su organización

Patricio Ramón
Socio de Risk Assurance
patricio.ramon@pwc.com

Fernando Fernández
Senior Manager Digital Risk
fernandez.fernando@pwc.com